An Intrusion Detection System with Active Response Generation

Levent Özgür Özalp, Ali Ziya Alkar

Abstract— In this study an Intrusion Detection System (IDS) is designed as a network based intursion detection solution that monitors, detects and proactively responds. The system supports operation at the stealth bridge mode and requires no change at the network topology. The solution is capable of searching for intrusion signatures inside the packets that come from multiple network interfaces simultaneously and capable of analyzing and filtering packets on any or all directions of traffic. Unlike any other IDS solution, the system incorporates both the active and the proactive responses. The protocol stack that comes with the operating system is bypassed and the functionality of the protocol stack of the operating system is implemented as a part of the IDS. This novel feature increases the performance of our system. [1]

Keywords— Firewall, Intrusion Detection System, Misuse Detection, Network Security,

I. INTRODUCTION

The threaths in IT such as misuse, unauthorized access, denial of service and others, have similar naming conventions as the typical security problems in our daily lives. It is not surprising to see that many daily life security solutions have been adopted to the IT directly from human life. If someone wants to model the IDSs (Intrusion Detection System) to human life, the most popular example would be the security cameras. This modeling indeed, is a reverse engineering from human life like every other security solution in the IT.

Now, to have a better understanding of the IT security, let us step back and take a brief look at the security issues in human life. The security solution today, in human life is to lock all the doors and windows and try to understand who is at the door when the door bell rings. In short, it is a selective input/output mechanism. A good example of monitoring is a car or a house alarm. The monitoring (the IDS of the IT security) is supposed to detect a security

Ali Ziya Alkar is with the Hacettepe University, Department of Electrical Engineering, Beytepe, Ankara. (phone: +90 312 2977027; fax: +90 312 2992125; e-mail: alkar@ hacettepe.edu.tr).

Levent Ozgur Ozalp is with 4S Computer Systems, Ovecler, Ankara. (phone: +90 312 472 9000; fax: +90 312 242 2022).

CONTENT REMOVED

II. CONCLUSION

The performance test results discussed implies that both with its bandwidth performance and attack detection performance under load, the Alageyik IDS has performed well to be classified as an IDS with a good performance.

Alageyik IDS with its stealth bridge architecture, real time process capability and the misuse detection methodology has managed to analyze the network traffic in real time and filter out the packets with attack signatures. Unlike other IDS solutions, the system incorporates both the active and the proactive responses. The protocol stack that comes with the operating system is bypassed and the functionality of the protocol stack of the operating system is implemented as a unique feature of our IDS.

This study aimed to prove that the designed IDS is performing fast and successful, most importantly it also aimed to prove that an IDS having a different packet inspection technique ***and*** active response generation can still perform like a typical IDS. It also indicates that the reason for this kind of an architecture not being implemented in a typical IDS, is not about its performance or success, it is more about the natural tendency to adopt a security solution in human life to the IT with all its deficiencies.